



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,113	06/20/2003	Amit Raikar	200309309-1	7736
22879 7590 07/15/2008 HEWLETT PACKARD COMPANY P O BOX 272400, 3404 E. HARMONY ROAD INTELLECTUAL PROPERTY ADMINISTRATION FORT COLLINS, CO 80527-2400				
EXAMINER CERVETTI, DAVID GARCIA				
ART UNIT 2136		PAPER NUMBER		
NOTIFICATION DATE 07/15/2008		DELIVERY MODE ELECTRONIC		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM

mkraft@hp.com

ipa.mail@hp.com

# Office Action Summary

**Application No.**

10/600,113

**Applicant(s)**

RAIKAR ET AL.

**Examiner**

DAVID CERVETTI

**Art Unit**

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 12 May 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 April 2007 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/5508)
- 4) ☐ Interview Summary (PTO-413)
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_
- Paper No(s)/Mail Date \_\_\_\_\_

**DETAILED ACTION**

1. Applicant's arguments filed May 12, 2008, have been fully considered but they are not persuasive.
2. Claims 1-16 are pending and have been examined. Claims 17-20 have been canceled.

***Response to Amendment***

3. Regarding claims 17-20, the rejection is withdrawn since the claims have been canceled.
4. Regarding the added limitation, a further consideration of the cited art revealed that Schneier does in fact teach the feature, see below.

***Claim Rejections - 35 USC § 102***

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
6. **Claims 1-17 are rejected under 35 U.S.C. 102(a) as being anticipated by Schneier et al. (US Patent Application Publication 2002/0087882, hereinafter Schneier).**

**Regarding claim 1**, Schneier teaches

an integrated intrusion detection method comprising (**par. 37**):

- gathering information from a plurality of different types of intrusion detection sensors (**pars. 35-36, monitors and collects information from sensors**);

- processing said information, wherein said processing provides a consolidated correlation of said information (**pars. 64-65, analysis**);
- assigning a severity to said information based on an enterprise wide security policy (**par. 88-94, incidents have severity levels and responses correspond to severity levels**);
- assigning a response corresponding to said information (**pars. 87-88, determine response**) and corresponding to said severity (**par. 88-94, incidents have severity levels and responses correspond to severity levels**); and
- implementing said response (**pars. 87-88, initiates response**) according to said severity (**par. 88-94, incidents have severity levels and responses correspond to severity levels**).

**Regarding claim 8, Schneier teaches**

a computer usable storage medium having computer readable program code embodied therein for causing a computer system to implement intrusion detection instructions comprising (**par. 37**):

- a data collection module for receiving information from a plurality of different types of intrusion detection sensors, wherein said information indicates potential security issues (**pars. 35-36, monitors and collects information from sensors**);
- an information severity determination module for assigning a severity to said information based on an enterprise wide security policy (**par. 88-94,**

**incidents have severity levels and responses correspond to severity levels);**

- an integration module for integrating said information in a network application management platform (**pars. 64-65, analysis**);
- a reaction determination module for determining appropriate response to indication of said potential security issues (**pars. 87-88, determine response**) according to said severity (**par. 88-94, incidents have severity levels and responses correspond to severity levels**); and
- a reaction direction module for directing said response (**pars. 87-88, initiates response**) according to said severity (**par. 88-94, incidents have severity levels and responses correspond to severity levels**).

**Regarding claims 2 and 9**, Schneier teaches wherein said information includes intrusion detection alerts (**pars. 62-64, alerts**).

**Regarding claim 3**, Schneier teaches centrally tracking information associated with intrusion detection alerts from said plurality of different types of intrusion detection sensors (**pars. 35-36, monitors and collects information from sensors, pars. 63-64**).

**Regarding claim 4**, Schneier teaches wherein said tracking information associated with intrusion detection includes assigning severity assignments standardized across said plurality of different types of intrusion detection sensors (**pars. 21 and 42, prioritize, par. 105, modify priority of problem**).

**Regarding claim 5**, Schneier teaches wherein said intrusion detection alerts are correlated based upon various alert attributes (**pars. 88-94, alerts and links to possible responses**).

**Regarding claim 6**, Schneier teaches wherein said response conforms to an enterprise wide strategy (**par. 60, rules**).

**Regarding claim 7**, Schneier teaches managing said intrusion detection sensors (**par. 37, adaptive sensors, receive updates dynamically**).

**Regarding claim 10**, Schneier teaches wherein said integration module selects appropriate hooks in an intrusion detection system (**pars. 41-42, connecting through pipes**).

**Regarding claim 11**, Schneier teaches wherein said data collection module logs alerts from said plurality of different types of intrusion detection sensors (**pars. 35-36, monitors and collects information from sensors, pars. 63-64**).

**Regarding claim 12**, Schneier teaches wherein said alerts are provided by a simple network management protocol (SNMP), a system log and an application program interface (**par. 36, SNMP sensors, syslogs, SNMP traps**).

**Regarding claim 13**, Schneier teaches wherein said integration module includes analyzing a plurality of manners in which an alert can be provided and selecting the manner that is the most secure with the least dependencies in a communication path (**pars. 63, selecting alert method**).

**Regarding claim 14**, Schneier teaches wherein said integration module utilizes a network application management platform to log information (**pars. 58-60, SOCRATES**).

**Regarding claim 15**, Schneier teaches wherein: an open view operation simple network management protocol trap is utilized to handle simple network management protocol trap based alerts; an open view operation log file encapsulator handles system log based alerts; and an open view message interceptor handles application program interface propagated alerts with the help of an operation message mechanism (**par. 36, SNMP sensors, syslogs, SNMP traps**).

**Regarding claim 16**, Schneier teaches wherein a secure open view template configuration is utilized to log information and the one message group is configured for handling intrusion detection system alerts and another message group is configured for handling intrusion detection system errors (**pars. 106-108, diverse groups and individuals are configured to receive alerts**).

### ***Conclusion***

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Hackenberger et al. (US Patent Application Publication 2002/0184532) teaches multiple security modules providing alerts, Fischman et al (US Patent Application Publication 2003/0097588) teaches correlating security information from diverse sources for intrusion detection, Bruton, III et al. (US Patent Application Publication 2003/0145225) teaches a centralized intrusion detection system, Scheidell (US Patent Application Publication 2004/0098623) teaches an IDS gathering information from a plurality of different types of intrusion detection sensors; processing said information, wherein said processing provides a consolidated correlation of said information; assigning a response corresponding to said information; and implementing said response.

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

Art Unit: 2136

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

9. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID CERVETTI whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.

11. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

12. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/  
Examiner, Art Unit 2136

/Nasser G Moazzami/  
Supervisory Patent Examiner, Art Unit 2136